# THE DATA ENCRYPTION STANDARD: 20 YEARS LATER

## Remarks of Panelist

**William H. Murray**
**Deloitte & Touche, Information Systems Security**
**49 Locust Avenue, Suite 104, New Canaan, CT 06840**
**203-966-4769, whmurray@sprynet.com**

Aren't you all glad that DES has finally been broken so that we can go on to something really interesting like selecting its successor?

However, before we go too far, pehaps we should review the situation.

Has the cost of decrypting a DES-encrypted message fallen to zero? No, nor even close. One estimate places the cost of DESCHALL at 500,000 MIPS years. On the average this would mean a cost of 1,000,000 MIPs years per key. Certainly adequate for some, not to say many or most, applications.

Has the cost of a brute force attack against the DES fallen from 2^55 operations to 2^47, as John Markoff reported in the NY Times after Biham and Shamir published their invention of Differential Cryptanalysis. No. In the absence of beneficial use of the key, one cannot use Differential Cryptanalysis to infer its identity.

Has the cost of decrypting a message without the key fallen to equal the cost of encrypting it with the key. No, the ratio of decrypting without the key to encrypting with it is exactly where it was twenty years ago. (In the case of DESCHALL it was marginally lower because the attackers took advantage of the knowledge that the plaintext was ascii. )

Has the cost of decrypting a message without the key fallen to the value of the data? That is to say, is DES no longer efficient. Except in very special cases, not likely; The value of the RSA DES challenge was $10,000, unusually high for a message of its length, and the cost of the 500,000 MIPs years was unusually low. It is unlikely that the organizer would repeat the experiment with his own money, much less do it over and over again. While we might reasonably infer that a nation state can recover any message that it likes, we can equally well infer that they cannot recover every message that they might like.

Has the cost of attack against the DES fallen to the point that is cheaper than breaking fingers or suborning one of the parties to the data. Or, in other words, is cryptanalysis of the DES efficient.

Has the duration of attack fallen to the life of the data. Again, not likely. While the value of most data decreases with age, by definition, the life of a challenge is equal to the duration of the attack. The life of "Squeamish Ossifrage" was fifteen years, or fifteen years and eight months, depending upon your view. Most messages have a life measured in hours to days rather than weeks or months.

Has someone even recovered one key or one message? Yes, we now know that someone has recovered at least one key and one message. Does that mean that the DES is broken? While they have demonstrated how to organize large numbers of computers to perform a benign and public task, they do not appear to have learned anything in this demonstration that would dramatically reduce the cost of subsequent attacks. Niether have they demonstrated anything else that was not already generally known.

When the NBS published the request for proposals for DES, I argued that IBM should not propose LUCIFER or any Feistel algorithm. I argued, based upon history, that publishing an algorithm would likely shorten its life. More important I thought, was that it would diminish its value to IBM. Incidentally, I thought that the idea behind the standard was only one of interoperability.

While it was hardly likely that anyone was listening to me then, fortunately for all of us, cooler, brighter heads prevailed. Dr. Lewis Branscomb, who was the IBM Chief Scientist and who had come to IBM from NBS, understood what many of us have only come to understand later. That is, the fundamental strength of an algorithm is necessary but it is not sufficient for its wide acceptance. It is also necessary that collectively we know something about that strength that we can communicate to other people in such a way to create the necessary trust and confidence.

The role of the standard and the NBS was to make a statement about the strength and to give authority to that statement The statement about strength was that the cheapest known attack was an exhaustive attack against the key. Dr. Ruth M. Davis, Director of The Institute of Computer Sciences and Technology at NBS, signed up for the standard. Perhaps she was only naive and not as courageous as she appears in hindsight.

The statement was based in part upon 17 man-years of analysis done by IBM and unknown amount done by NBS and NSA. The NSA role was sponsored by Howard Rosenblum, Deputy Director, COMSEC, NSA, who led, not to say fought single-handedly, the only battle that COMSEC ever won over SIGINT.

Other heroes in my story include:

Robert H. Courtney, Manager of Data Security for IBM's Systems Development Division, godfather of the DES, who understood that you could not do automated teller operations offline or in the clear. and who wrote the original encryption criteria given to IBM Research

Dr. Arthur Anderson, Director of Research at IBM, who funded the original research on not much more than an assertion that it would be good for computer security.

Horst Feistel, the father of the whole class of algorithms of which DES was a member and the godfather, if not the inventor of complexity-based cryptography.

Walter Tuchman, who led the team that produced the DES and the IBM products based upon it.

Seymour Jeffery and Dennis Branstead, who did the technical work for NIST, along with Doug Hogan of NSA.

Whitfield Diffie and Martin Hellman, the DES' public critics whose calculations contributed to our understanding of its strength and limitations. They predicted that the 56 bit key would one day prove to be too short for some applications. While I think that they visualized a DES cracking machine, they did predict that it would prove too short in the context of a massively parallel attack.

We are indebted also to Don Coppersmith, K. W. Campbell, and Michael Wiener for proving that DES is composable (i.e., DES is not a Group) and to the IBM teams that told us how to do it safely.

The hedge on the standard statement was that we only expected it to have to last for five years; we could not even bring ourselves to hope that it would still be true twenty years later. While we could not forsee that anyone would ever be able to organize thousands of computers in different organizations and even nations into such an effort as DESCHALL, we could forsee massively parallel attacks.

The IBM team did not worry much about such attacks any more than they worried about the 56 bit key length. They always knew what they were going to do about it. While everyone else was busy calculating the cost of a brute force attack against a 56 bit key, they were busy exploiting the ideas that one cannot do a plaintext-only attack against a randomly chosen key nor an efficient attack against a session or message key. The IBM 3848 used Triple-EDE-112 in 1979.

Courtney's first law reminds us that nothing can be said about the security of a mechanism except in the context of a specific application and environment. In that context, I will continue to prefer the DES and its implementations and compositions to all other algorithms unless and until the standard measure, i.e., the cheapest known attack is an exhaustive attack against the key, is no longer a valid statement. While I will consent to the use of alternatives, as a professional, I will not recommend them.

Today the DES is a *de facto* as well as a *de jure* standard. It is a *de facto* standard because of the fruits of twenty years of research. After due consideration, every report that the DES has been broken has led to a new appreciation of its strength.

In order for a new *de jure* standard to be preferred to the DES, it will have to overcome the advantage that DES gets from that knowledge. It is not sufficient that the new algorithm has a longer key length or appears to be more complex, than the DES. We must know about it with the same degree of confidence that we know about the DES.

So, while twenty years ago we could not predict that the DES would stand for twenty years, today we can safely predict that it is timeless. While one can hypothesize applications and environments for which it is not adequate, we do not have any problems like that in the real world. For all real world problems we know how to use it, compose it, and manage it's keys so as to compensate for its limitations.